تكوين نشر TrustSec SGT SXP في SD-WAN

المحتويات

المقدمة

يصف هذا المستند تكوين طريقة نشر بروتوكول تبادل علامات مجموعة الأمان (SXP) في الشبكات الواسعة المحددة للبرامج (SD-WAN).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة منطقة واسعة معرفة ببرنامج Cisco Catalyst (SD-WAN)
- قناة الوصول المعرفة عن طريق البرامج (SD-ACCESS) الليفية
- محرك خدمة التحديد (ISE) من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى:

- Cisco IOS® XE Catalyst SD-WAN Edges ، الإصدار 17.9.5a
- Cisco Catalyst SD-WAN Manager، الإصدار 20.12.4.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تكامل Cisco TrustSec

يتم دعم نشر أداة Sgt مع تكامل Cisco TrustSec بواسطة Cisco IOS® XE Catalyst SD-WAN الإصدار 17.3.1a وما بعده. تمكن هذه الميزة أجهزة Cisco IOS® XE Catalyst SD-WAN edge لنشر علامات مجموعة الأمان (SGT) المضمنة التي يتم إنشاؤها بواسطة محولات Cisco TrustSec التي تم تمكينها في الفروع إلى أجهزة الحافة الأخرى في شبكة Cisco Catalyst SD-WAN.

المفاهيم الأساسية ل Cisco TrustSec:

- الربط بين بينين: الاقتران بين IP و SGT، تتم جميع الروابط بالتكوين الأكثر شيوعا، كما تتعلمها مباشرة من Cisco ISE.
- انتشار الربط: ويتم إستخدام طرق النشر لنشر هذه الربط بين الشبكة.
- جه SGTACLs: مجموعة من القواعد التي تحدد امتيازات مصدر حركة مرور داخل شبكة موثوق بها.
- تنفيذ الربط: عندما يتم فرض السياسات، فإن ذلك يعتمد على سياسة الربط.

أساليب نشر الربط

طرق نشر الربط هي:

- وضع علامات على الخط الداخلي لنشر الربط
- نشر الربط SXP

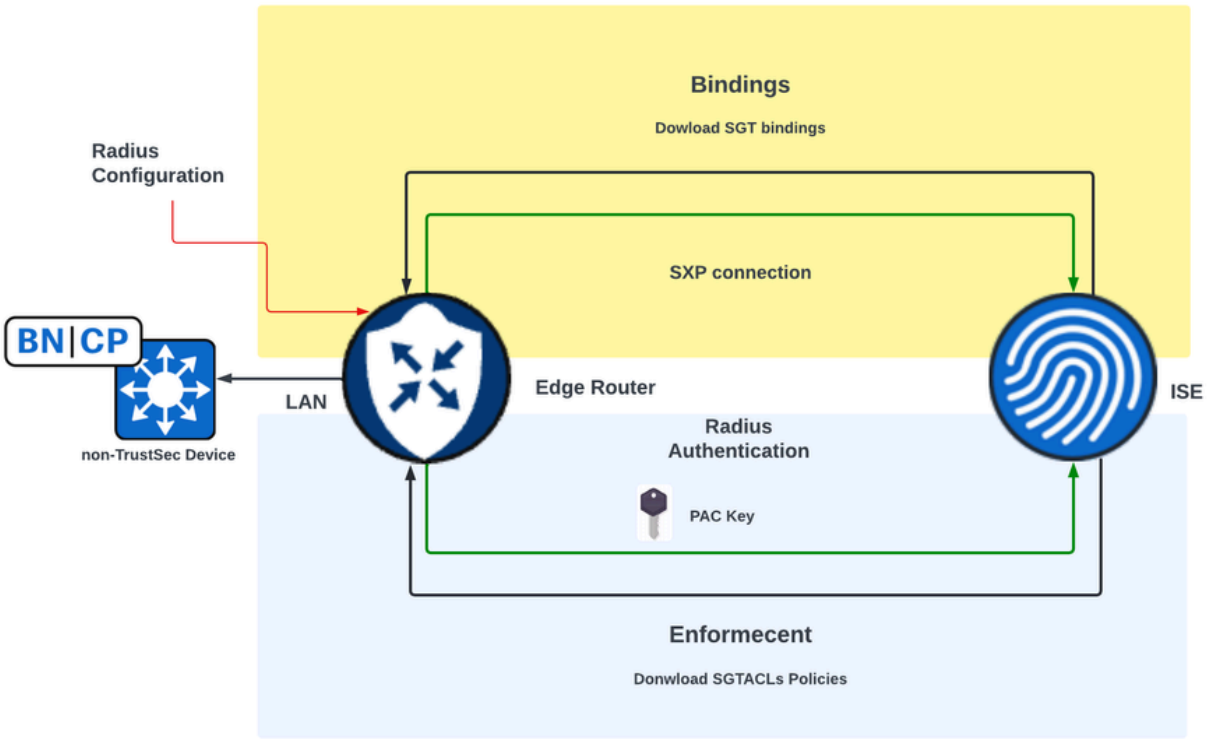
نشر الربط مع SXP

بالنسبة لنشر العلامات عبر الإنترنت، يجب تزويد الفروع بمحولات Cisco TrustSec التي تم تمكينها والتي يمكنها معالجة وضع العلامات SGT لخاد السطر (أجهزة Cisco TrustSec). إذا كان الجهاز لا يدعم وضع العلامات لخاد الجهاز، فإن نشر الربط يستخدم بروتوكول لدابت علامات مجموعة الأمان (SXP) لنشر الربط عبر أجهزة الشبكة.

يسمح Cisco ISE بإنشاء ربط IP-to-SGT (IP-SGT ديناميكي) ثم يقوم بتنزيل ربط IP-SGT باستخدام SXP إلى جهاز Cisco IOS® XE Catalyst SD-WAN لنشر الربط عبر شبكة Cisco Catalyst SD-WAN. أيضا، يتم فرض سياسات حركة مرور الربط على مخرج SD-WAN من خلال تنزيل سياسات SGACL من ISE.

مثال:

- ال يدعم محول Cisco (العقدة الحدودية) وضع العلامات في السطر (جهاز غير TrustSec).
- يسمح Cisco ISE بتنزيل ربط IP-SGT من خلال اتصال SXP بجهاز Cisco IOS® XE Catalyst SD-WAN (هجوم الحافة).
- يسمح Cisco ISE بتنزيل سياسات SGACL من خلال تكامل RADIUS ومفتاح PAC إلى جهاز Cisco IOS® XE Catalyst SD-WAN (هجوم Edge).

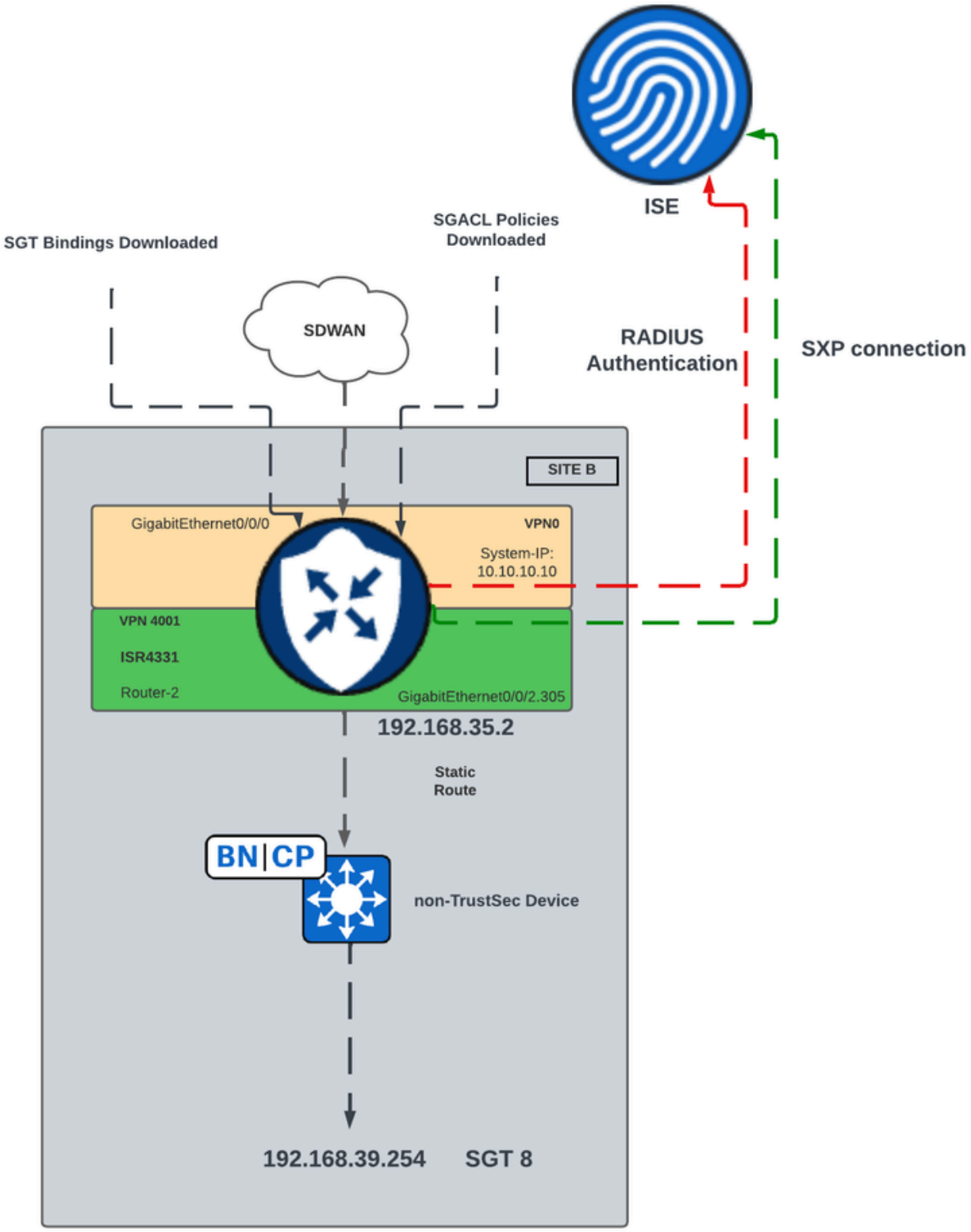


متطلبات تمكين نشر SXP وتنزيل سياسات SGACL على أجهزة SD-WAN الطرفية

ملاحظة: لا يتم فرض سياسات SGACL على حركة مرور الدخول، فقط على حركة مرور الخروج في شبكة Cisco Catalyst SD-WAN.

ملاحظة: ميزة Cisco TrustSec غير مدعومة لأكثر من 24 ألف نهج من سياسات الرقيب في وضع وحدة التحكم.

تمكين نشر SXP وتنزيل سياسات SGACL

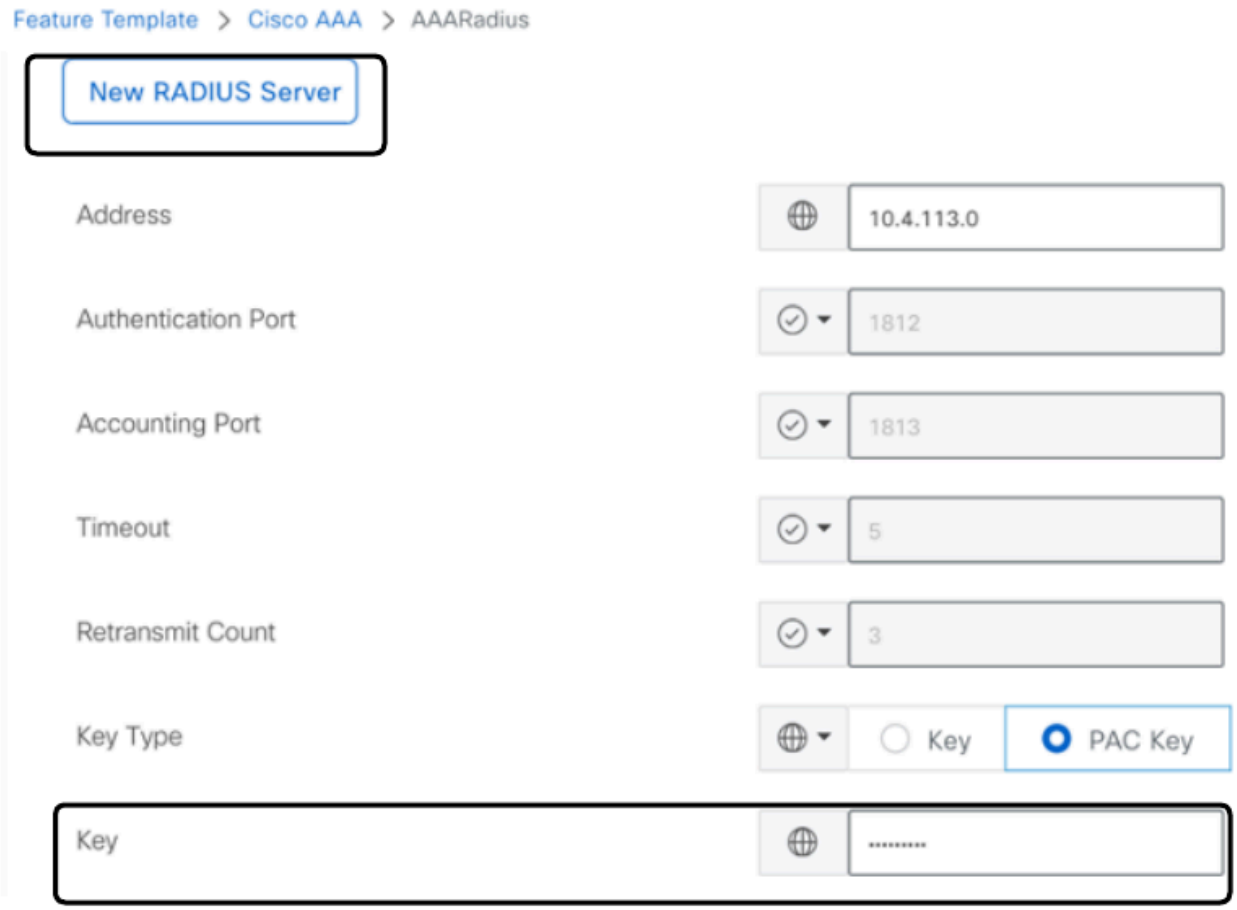


الرسم التخطيطي للشبكة لعملية النشر Sgt SXP في SD-WAN

الخطوة 1. تكوين معلمات RADIUS

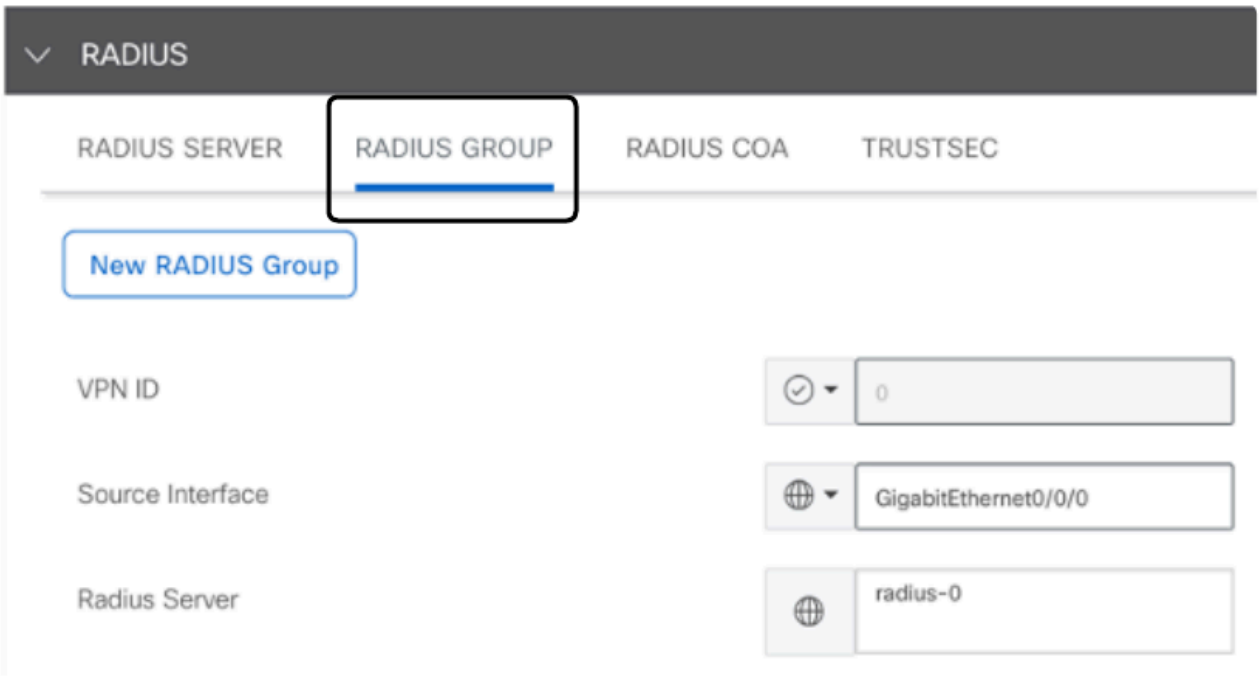
- سجل الدخول إلى واجهة المستخدم الرسومية Cisco Catalyst SD-WAN Manager.
- انتقل إلى التكوين > قوالب > قالب الميزة > Cisco AAA. انقر فوق خادم RADIUS.

- قم بتكوين معلمات خادم RADIUS والمفتاح.



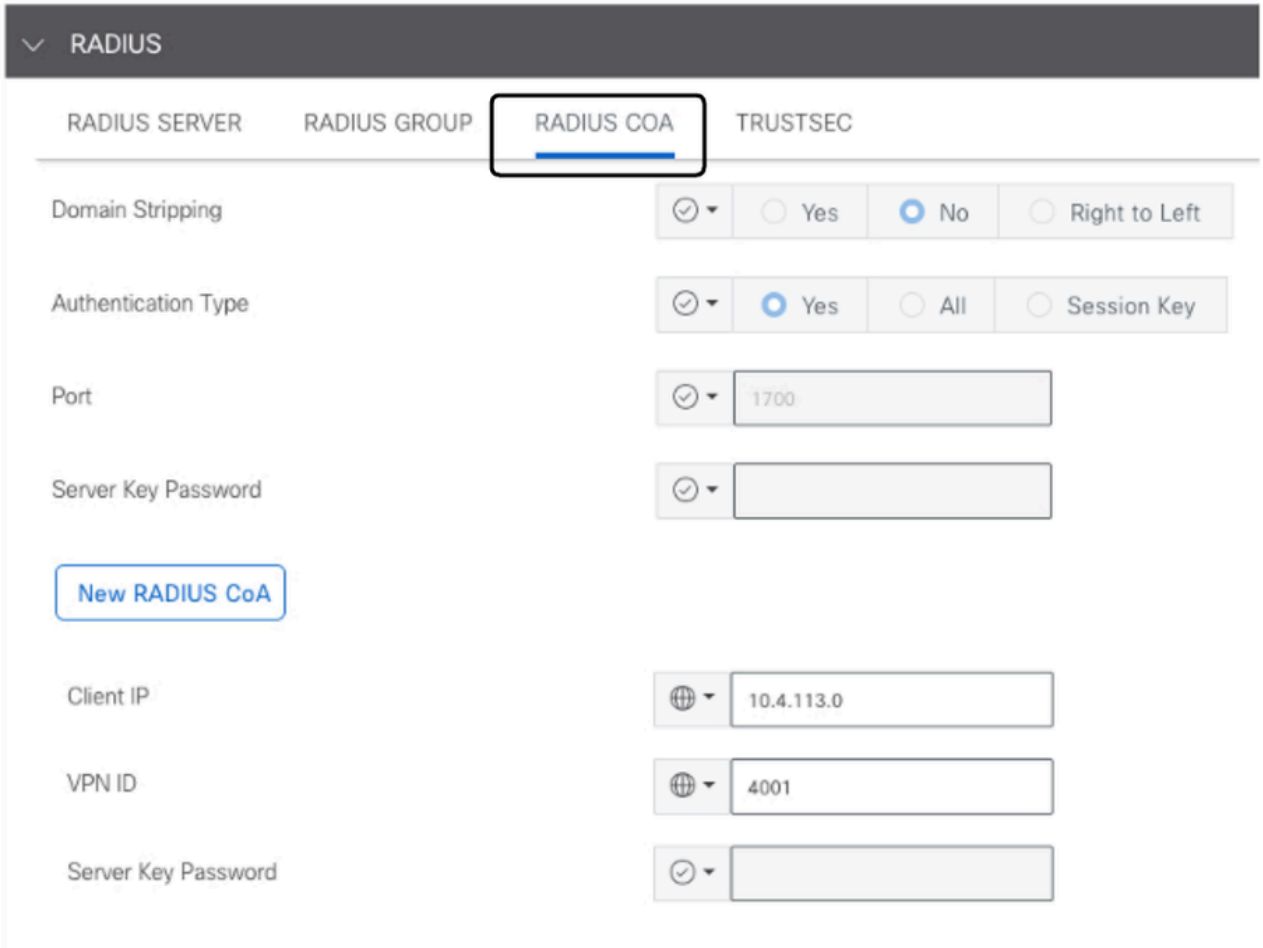
تكوين خادم RADIUS

- أدخل القيم لتكوين معلمات مجموعة RADIUS.



تكوين مجموعة RADIUS

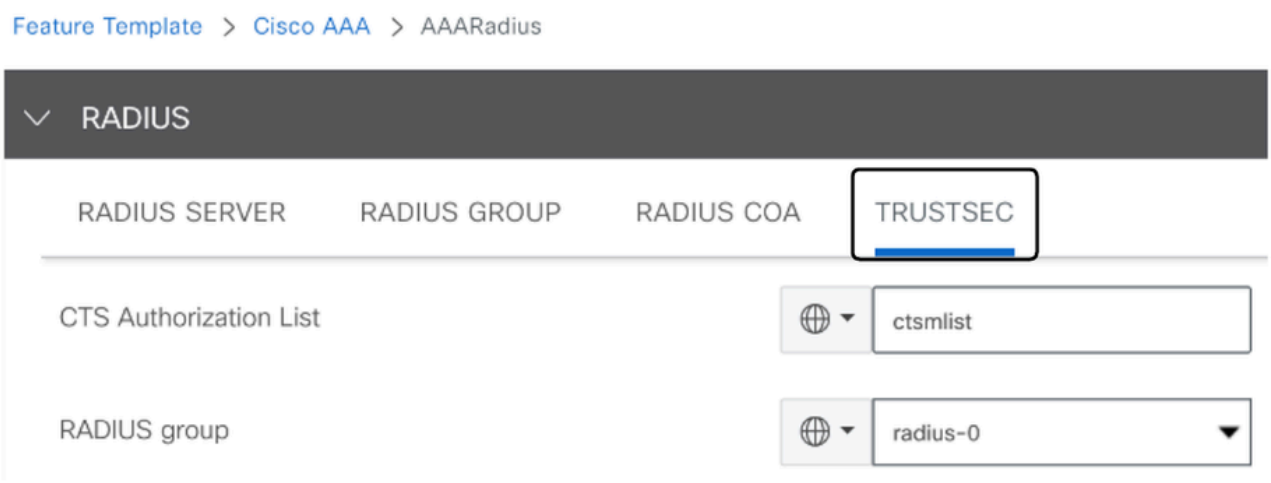
- أدخل القيم لتكوين معلمات RADIUS COA.



تكوين RADIUS COA

ملاحظة: إذا لم يتم تكوين RADIUS COA، فلن يتمكن موجه SD-WAN من تنزيل سياسات SGACL تلقائيا. بعد إنشاء نهج SGACL من ISE أو تعديله، يتم إستخدام الأمر cts refresh policy لتنزيل السياسات.

- انتقل إلى قسم TRUSTsec وأدخل القيم.

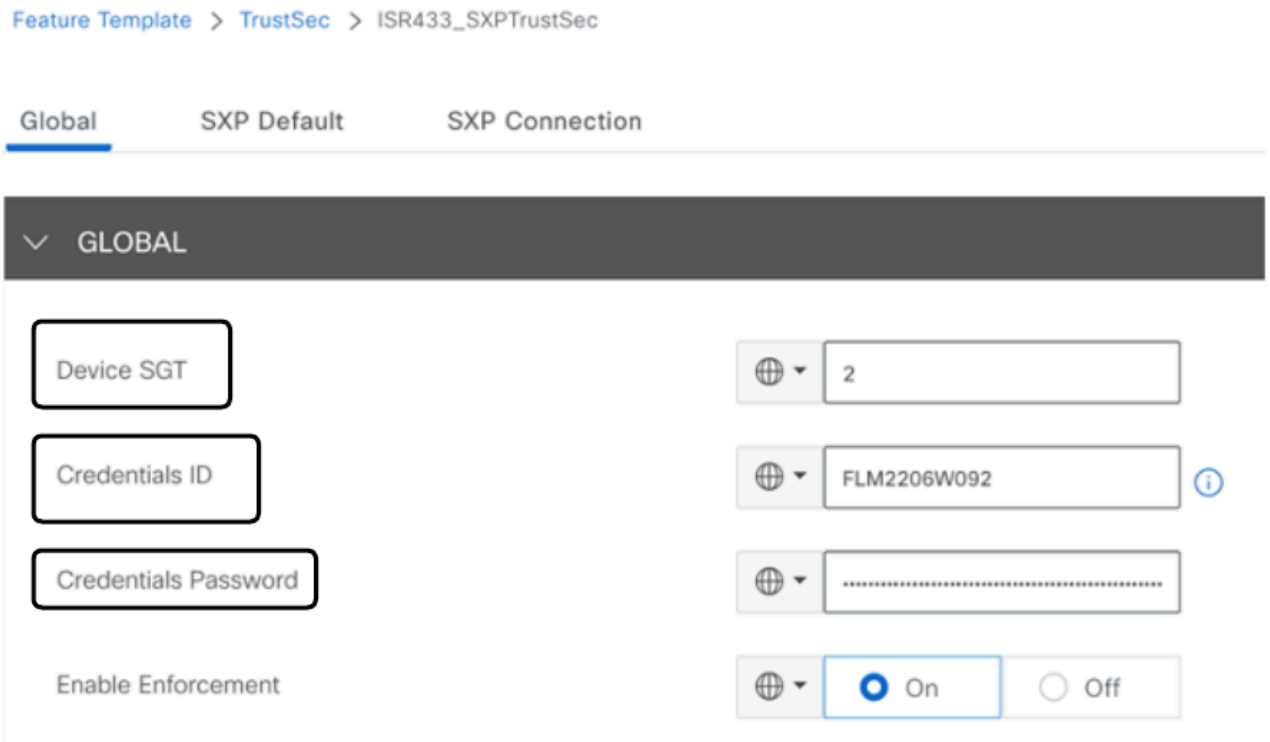


تكوين TRUSTsec

- قم بإرفاق قالب ميزة Cisco AAA بقالب الجهاز.

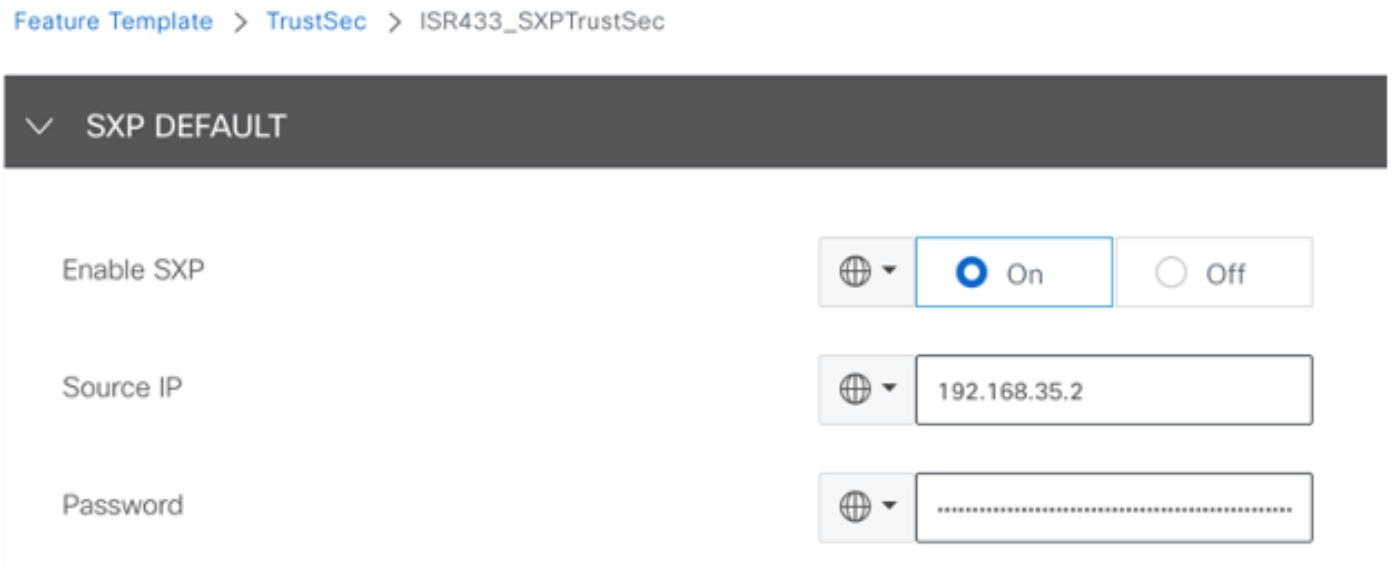
الخطوة 2. تكوين معلمات SXP

- انتقل إلى التكوين > القوالب > قالب الميزات > TrustSec.
- قم بتكوين بيانات اعتماد CTS وعينت ربط SGT لواجهات الجهاز.



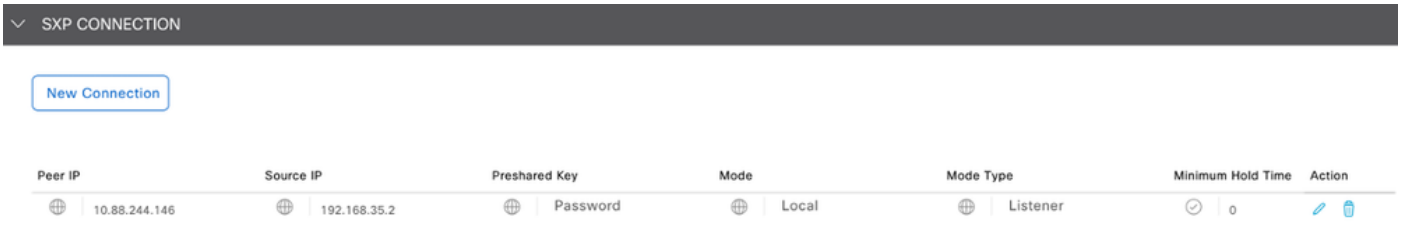
قالب ميزة TrustSec

- انتقل إلى قسم SXP الافتراضي وأدخل القيم لتكوين معلمات SXP الافتراضية.



التكوين الافتراضي ل SXP

- انتقل إلى اتصال SXP وشكلت معلمات اتصال SXP، ثم انقر على حفظ.

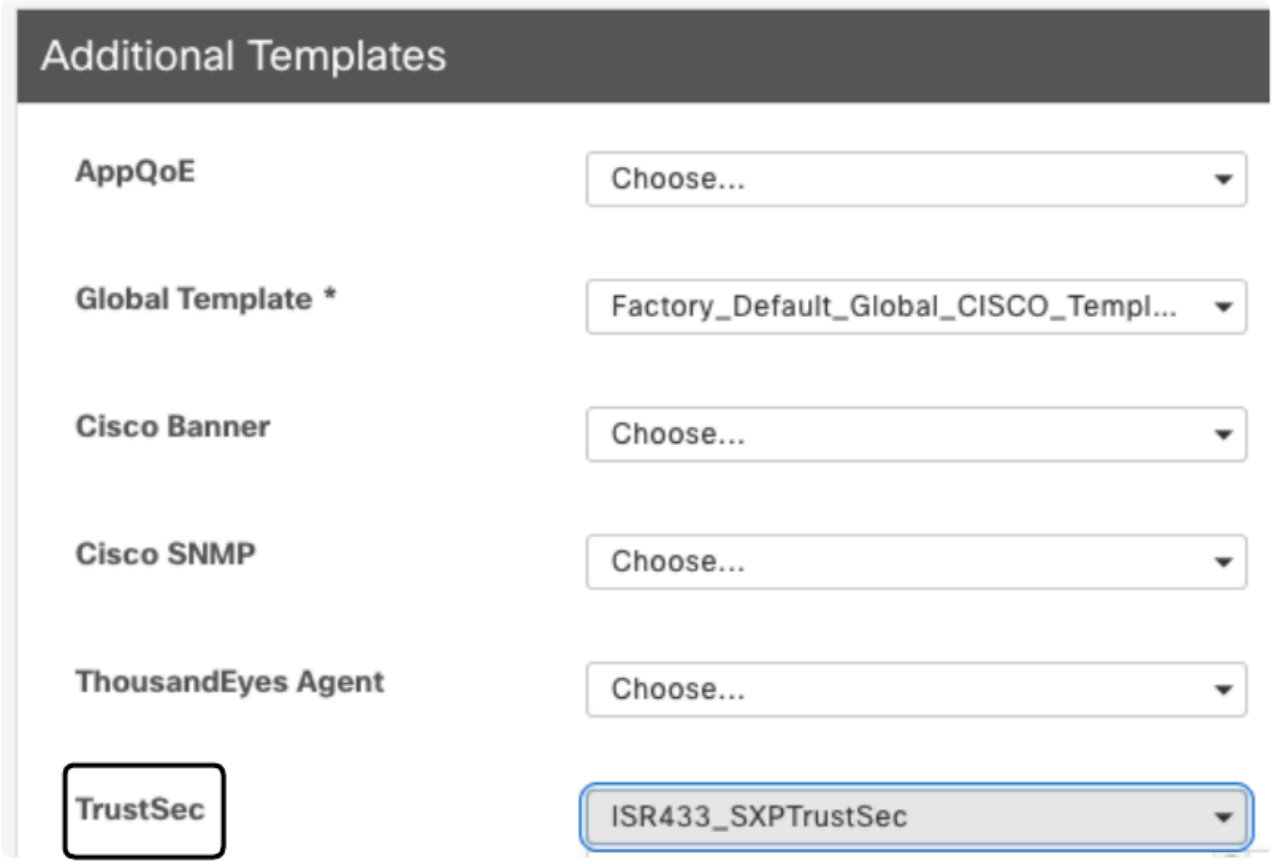


تكوين اتصال SXP

ملاحظة: يحتوي Cisco ISE على حد على عدد جلسات عمل SXP التي يمكنه معالجتها. لذلك، كبديل، يمكن إستخدام عاكس SXP لقياس الشبكة الأفقية.

ملاحظة: يوصى باستخدام عاكس SXP لإنشاء نظير SXP باستخدام أجهزة Cisco IOS® XE Catalyst SD-WAN.

- انتقل إلى التكوين > قوالب > قالب الجهاز > قوالب إضافية > TrustSec.
- حدد قالب ميزة TrustSec الذي تم إنشاؤه مسبقا، انقر فوق حفظ.



قسم القوالب الإضافية

التحقق من الصحة

قم بتشغيل الأمرshow cts sxp connections vrf (service vrf)لعرض معلومات إتصالات Cisco TrustSec SXP.

<#root>

#show

cts

sxp

connections

vrf

4001

SXP : Enabled

```
Highest Version Supported: 5
Default Password : Set
Default Key-Chain: Not Set
Default Key-Chain Name: Not Applicable
```

```
Default Source IP: 192.168.35.2
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
```

Peer IP : 10.88.244.146

Source IP : 192.168.35.2

Conn status : On

```
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Hold timer is running
```

Total num of SXP Connections = 1

قم بتشغيل الأمر **show cts role-based sgt-map** to عرض خريطة الرقيب العامة Cisco TrustSec بين عنوان IP وربط الرقيب.

<#root>

#

show

cts

role-based

sgt

-map

vrf

4001 all

```
Active IPv4-SGT Bindings Information
IP Address              SGT     Source
============================================
192.168.1.2             2       INTERNAL
192.168.35.2            2       INTERNAL
```

192.168.39.254 8 SXP <<< Bindings learned trough SXP for the host connected in the

```
IP-SGT Active Bindings Summary
```

```
==========================================
Total number of CLI      bindings = 0
Total number of SXP      bindings = 1

Total number of INTERNAL bindings = 2
Total number of active   bindings = 3
```

قم بتشغيل الأمر **show cts environment-data** لعرض بيانات بيئة Cisco TrustSec العامة.

```
<#root>
#show
cts
 environment-data

CTS Environment Data
====================
Current state = COMPLETE

Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-01:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 1 server(s):
 Server: 10.88.244.146, port 1812, A-ID B546BF54CA5778A0734C8925EECE2215
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

Security Group Name Table:

    0-00:Unknown

    2-01:TrustSec_Devices

    3-00:Network_Services

    4-00:Employees

    5-00:Contractors

    6-00:Guests
```

```
    7-00:Production_Users

    8-02:Developers
          <<<<< Security Group assigned to the host connected in the LAN side (SGT 8)
    9-00:Auditors

    10-00:Point_of_Sale_Systems

    11-00:Production_Servers

    12-00:Development_Servers

    13-00:Test_Servers

    14-00:PCI_Servers

    15-01:BYOD

Environment Data Lifetime = 86400 secs
```

قم بتشغيل الأمرshow cts pacsلعرض مسوغات الوصول المحمي (PAC) المزودة من Cisco TrustSec.

```
<#root>
#show cts pacs

AID: B546BF54CA5778A0734C8925EECE2215
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: B546BF54CA5778A0734C8925EECE2215
  I-ID: FLM2206W092

A-ID-Info: Identity Services Engine
  Credential Lifetime: 22:24:54 UTC Tue Dec 17 2024
```

```
PAC-Opaque: 000200B800030001000400010B546BF54CA5778A0734C8925EECE22150006009C00030100BE30CE655A7649A5CED8
```

قم بتشغيل الأمرshow cts role-based permissions to عرض جميع SGACL.

```
<#root>

#show

cts

 role-based permissions


IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group 2:TrustSec_Devices:
        Deny IP-00

IPv4 Role-based permissions from group 5:Contractors to group 8:Developers:



DNATELNET-00


IPv4 Role-based permissions from group 5:Contractors to group 15:BYOD:
        Deny IP-00
```

قم بتشغيل الأمرshow cts rbacl (SGACLName)لعرض تكوين قائمة التحكم في الوصول (SGACL).

```
<#root>

#show

cts


rbacl

 DNATELNET


CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =

DNATELNET-00


  IP protocol version = IPV4, IPV6
  refcnt = 2
  flag   = 0xC1000000
  stale  = FALSE
```

```
RBACL ACEs:


    deny
tcp


dst
 eq 23 log
       <<<<< SGACL action
    permit
ip
```

معلومات ذات صلة

- دليل تكوين أمان Cisco Catalyst SD-WAN
- دليل تكوين Cisco TrustSec

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).